Amendments to the Claims

Claim 1 (Currently amended): A system ~~(100)~~ for processing data, the system comprising encrypted first data from a first user, and encrypted second data from a second user,

a server ~~(150)~~ configured to obtain the encrypted first and second data, the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second users to each other,

computation means ~~(110, 150,190, 191,199) for performing a computation on the encrypted first and second data~~ to obtain a similarity value between the first and second data, said computation comprising directly calculating either an encrypted inner product between the first and second data or an encrypted sum of shares of the first and second data,

wherein ~~so that~~ the first and second data is anonymous to the second and first users respectively, the similarity value providing an indication of a similarity between the first and second data.

Claim 2 (Previously presented): The system of claim 1, wherein the second user calculates, through computational means, an encrypted inner product between the first data and the second data, and provides the encrypted inner product to the first user via the server, the first user decrypting the encrypted inner product for obtaining the similarity value through computational means.

Claim 3 (Original): The system of claim 1, wherein the computation means is realized using a Paillier cryptosystem, or a threshold Paillier cryptosystem using a public key-sharing scheme.

Claim 4 (Original): The system of claim 1, wherein the server comprises the computation means to obtain an encrypted inner product between the first data and the second data, or encrypted sums of shares of the first and second data in the similarity value, and the server is coupled to a public-key decryption server for decrypting the encrypted inner product or the sums of shares and obtaining the similarity value.

Claim 5 (Previously presented): The system according to anyone of claim 1, wherein the similarity value is obtained using a Pearson correlation or a Kappa statistic.

Claim 6 (Currently amended): A method of processing data, the method comprising steps of enabling to:

~~- (210)~~ encrypt first data for a first user, and encrypt second data for a second user[[,]];

~~- (220)~~ provide the encrypted first and second data to a server that is precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second user to each other[[,]];

~~- (230)~~ perform a computation on the encrypted first and second data to obtain a similarity value between the first and second data, said computation comprising directly calculating either an encrypted inner product between the first and second data or an encrypted sum of shares of the first and second data; and

wherein ~~so that~~ the first and second data is anonymous to the second and first users respectively, the similarity value providing an indication of a similarity between the first and second data.

Claim 7 (Previously presented): The method of claim 6, wherein the first or second data comprises a user profile of the first or second user respectively, the user profile indicating user preferences of the first or second user to media content items.

Claim 8 (Original): The method of claim 6, wherein the first or second data comprises user ratings of respective content items.

Claim 9 (Currently amended): The method of claim 6, further comprising a step ~~(240)~~ of using the similarity value to obtain a recommendation of a content item for the first or second·user.

Claim 10 (Original): The method of claim 9, wherein the recommendation is performed using a collaborative filtering technique.

Claim 11 (Currently amended): A server ~~(150)~~ for processing data,

the server being configured to obtain encrypted first data of a first user ~~(110)~~ and encrypted second data of a second user~~(190,191, 199)~~,

the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second users to each other,

enable a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first users respectively, said computation comprising directly calculating either an encrypted inner product between the first and second data or an encrypted sum of shares of the first and second data,

wherein the similarity value providing an indication of a similarity between the first and second data.

Claim 12 (Currently amended): A method of processing data, the method comprising steps of

~~—(220)~~ obtaining encrypted first data of a first user ~~(110)~~ and encrypted second data of a second user ~~(190,191, 199)~~ by a server ~~(150)~~, the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second users to each other,

~~—(230)~~ enabling a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first users respectively, said computation comprising directly calculating either an encrypted inner product between the first and second data or an encrypted sum of shares of the first and second data,

wherein the similarity value providing an indication of a similarity between the first and second data.

Claim 13 (Currently amended): A computer readable medium being structured so as to comprise:

an indication of similarity between an encrypted first data and an encrypted second data by receiving encrypted first data from a first user and encrypted second data from a second user; and,

performing a computation on the encrypted first and second data so that the first and second data is anonymous to the second and first users respectively

wherein said computation comprises directly calculating either an encrypted inner product between the first and second data or an encrypted sum of shares of the first and second data.